

Claims

1. A network device for implementing IPSec and comprising:
 - at least one IP forwarder arranged to receive IP packets each of which is associated with a Security Association (SA), to determine the destinations of the packets, and to forward the packets to their destinations;
 - a plurality of security procedure modules coupled to the IP forwarder(s) and arranged to implement security procedures for received IP packets in parallel; and
 - a security controller arranged to allocate negotiated SAs amongst the security procedure modules and to notify the security procedure modules and the IP forwarder(s) of the allocation, whereby the IP forwarder(s) can send IP packets to the security procedure module implementing the associated SA.
2. A device according to claim 1, wherein the security procedure modules are coupled together to allow the forwarding of an IP packet from one security procedure module to another.
3. A device according to claim 1, wherein the security controller is responsible for creating and modifying IP packet filters in the IP forwarder(s), wherein the filters are responsible for routing IP packets to the security procedure modules.
4. A device according to claim 3, wherein the filtering of packets is carried out using one or more selectors, the or one of the selectors being the Security Parameter Index (SPI) which identifies a SA and which is contained in a header of the IP packets.
5. A device according to claim 1, wherein the security controller is coupled to an Internet Key Exchange (IKE) module which is responsible for negotiating SAs with peer IKE modules, and the security controller is arranged to receive from the IKE module details of negotiated SAs.
6. A device according to claim 1, wherein the IP forwarder(s), security procedure modules, and/or security controller are implemented in software or in hardware, or in a combination of hardware and software.

7. A method of processing IP packets at a network networking device, the method comprising:

allocating negotiated SAs amongst a plurality of security procedure modules arranged to implement security procedures for received IP packets;

notifying the security procedure modules and at least one IP forwarder of said allocation; and

receiving IP packets at the IP forwarder(s), identifying the SAs associated with the packets, and forwarding the packets to the security procedure modules implementing the associated SAs.